C.1 BACKGROUND

Cyber attacks on Federal networks are growing in numbers and becoming increasingly sophisticated, aggressive and dynamic. In 2011, the Federal Government responded to more than 107,000 attacks including cyber exploits that injected viruses, stolen information, or disrupted Federal network operations. In contrast, the decade old security regulations require manually testing major systems just once every three years, resulting in compilation of three-ring binder findings that are often out of date before they can be printed.

The security community recognized several years ago that a static approach to information assurance was inadequate. Since that time, the Federal Government has initiated a number of activities under the title "Continuous Monitoring" to improve the situation. Accordingly, various approaches toward continuous monitoring are being developed by agencies.

There are different levels of maturity in continuous monitoring across the Federal enterprise. The different approaches complicate the efforts to measure progress on a Federal enterprise level. Several Federal agencies have had isolated success. In 2008, the Department of State began a program to utilize sensors, in combination with a dashboard solution, to identify and fix cyber vulnerabilities on their networks. This program achieved a dramatic measured risk reduction (in terms of system vulnerabilities) of 20 times in just two years. Leveraging this success, the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program is strongly influenced by the State Department program. The DHS Continuous Diagnostics and Mitigation (CDM) program provides tested continuous monitoring, diagnosis, and mitigation capabilities designed to strengthen the security posture of the Federal civilian .gov networks.

The objective of the CDM dashboard function is to provide consistent, timely, targeted, and prioritized information to security decision-makers from cross-department, agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first. The goal is to mitigate these risks before they can be exploited and cause harm to the Department and Agency (D/A) IT assets, business assets, or mission. The objectives of the CDM Dashboard initiative will be achieved by:

1. Receiving/collecting data from the D/A-level dashboards.
2. Facilitating the risk management process.
3. Reporting results to appropriate officials through a web-based user interface, organizationally-defined reports, and ad hoc query and reporting tools.

Federal Information Security Management Act (FISMA) compliance reporting mandated by the Office of Management and Budget (OMB) can be achieved through the use of Asset Summary Results (ASR) and Security Content Automation Program (SCAP) protocols for IT asset information as defined by the National Institute of Standards and Technology (NIST). The D/As will establish the communication between the Federal Level CDM Dashboard and Dashboards at other levels to report enterprise security posture information using an ASR-encapsulated summary of results.

The Dashboards will be used to automate FISMA compliance reporting mandated by OMB, including reporting through CyberScope. This reporting can be achieved through the use of NIST-defined ASR and SCAP protocols for IT asset information. The D/As will use the communication between the D/A Level and Federal Level Dashboards to report enterprise security posture information using an ASR-encapsulated summary of results. The CDM Dashboard solution will be Sensitive but Unclassified (SBU) and must be accredited as High Confidentiality, High Integrity, and Moderate Availability.

C.1.1 PURPOSE

Under the CDM program, DHS will centrally oversee the procurement, operations, and maintenance of diagnostic sensors (tools) and dashboards deployed to each agency. Using input from the sensors and agency-level CDM dashboards, Officials at each agency will be able to quickly identify which problems to fix first and empower technical managers to prioritize and mitigate risks. In addition, DHS will maintain a Federal level CDM Dashboard taking input from the agency-level dashboards, to provide situational awareness on a Federal level.

Under this procurement, GSA on behalf of DHS is commissioning the creation of an IT solution known as the "CDM Dashboard." To that end, this procurement will obtain software design and development services and software/hardware for a series of Dashboard releases, or instances. DHS has the further strategic goal of implementing the completed CDM Dashboard use cases to other Federal agencies to manage and report their vulnerability to cyber-attacks; however, the only implementation in scope of this procurement is the Federal use case. The Dashboard created under this procurement will be used to automate FISMA compliance reporting mandated by OMB, including reporting through the currently used FISMA reporting tool, CyberScope. The Contractor shall design, develop, and support the Federal implementation of the Dashboard solution. Implementation (of the CDM Dashboard solution developed under the efforts of this procurement) at individual D/As implementation will be handled by CMaaS vendors in separate acquisitions. While the actual integration will not be performed under this task order, the contractor shall provide on-going support to CMaaS vendors to maintain and improve the functional processes within Dashboard software, to include: analysis, DHS system engineering lifecycle (SELC) reviews, software development, testing, security accreditation support, implementation support (to include acquiring property), maintenance, documentation, configuration management, Tier 3 support, training, customer relationship management, transition to support, and acquisition milestone tracking. The progression of the functionality of the Dashboard under this Task Order will be done incrementally over multiple software releases.

C.1.2 AGENCY MISSION

For this specific acquisition, the DHS strategic goal is to purchase an integrated, hierarchical Dashboard solution, to implement the Federal use case, and to make the Dashboard capability available to DHS and Federal agencies to manage and report their vulnerability to cyber-attacks.

C.1.3 CDM Dashboard Terminology and Architecture

This section describes the dashboard's terminology and includes an architectural diagram of the proposed dashboard hierarchy. This terminology will be used throughout this Task Order Request and during the execution of these requirements.

C.1.3.1 CDM Dashboard Terminology

DASHBOARD

The term *Dashboard* is used in the context of the CDM Program to refer to all parts of the Continuous Asset Evaluation, Situational Awareness and Risk Scoring Reference Architecture Report (**CAESARS**) architecture except the sensor sub-system. The CAESARS was published by DHS in 2010 and available at http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf. The term Dashboard addresses the remaining parts of the CAESARS architecture: Database/Repository, Analysis/Risk Scoring, and Presentation and Reporting. CDM dashboards are arranged in a hierarchy. Each dashboard will be an independently executing application with its own inputs and outputs. The dashboards may be technically equivalent but will function differently based on their position in the hierarchy. DHS will deploy a hierarchical CDM Dashboard solution at DHS and at the D/As. There are four tiers of dashboard deployment, corresponding to four hierarchy locations. Those D/As that currently have existing legacy applications that are also known as "dashboards" but provide functionality not specific to CDM capabilities will be able to keep them but will also be required to utilize the CDM Dashboard solution. Existing D/A legacy dashboards are unrelated to this effort. The CDM Dashboard assumes that all data it receives is normalized and SCAP compliant. It is the responsibility of the sensor layer within the CAESARS Framework to perform this function.

The **Federal Level CDM Dashboard** displays summary CDM data for the entire Federal Government. This dashboard will be used by oversight groups, e.g., Offices of Inspector Generals, to monitor Government-wide risk. Implementation of this CDM Dashboard will be the responsibility of the CDM Dashboard vendor.

An **Intermediate Summary CDM Dashboard** is an instance of the DHS-provided D/A solution that obtains all of its data from other D/A dashboards, and all of whose data is at a summary level (no object-level data). Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

Only other Summary CDM Dashboards and/or the Federal Level CDM Dashboard may exist above this level in the hierarchy. This type of dashboard would be used to summarize data for a large D/A where object-level data is not required/ permitted.

An **Intermediate Object-Level CDM Dashboard** is an instance of the DHS-provided D/A solution that obtains all of its data from other D/A dashboards, but some of whose data is at the object level.

Only base (see below) and/or other Intermediate Object-Level Dashboards may exist below this dashboard. This type of dashboard would be used if multiple Base Dashboards are needed (for performance reasons, for example) for a D/A, and the D/A still wants/permits detailed data at the D/A level. It can have all the functionality of a Base CDM Dashboard except that which requires connection to sensors. (Functionality related to these missing items is turned off).

In general, Intermediate-level dashboards are for use by D/As and/or their sub-components to monitor the risk associated with their organizational scope. If the dashboard is object-level, then it will also facilitate identification and removal of specific defects on specific objects. Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

A **Base CDM Dashboard** is an instance of the DHS-provided D/A solution whose data is obtained directly from sensors. Each Base CDM Dashboard must be capable of obtaining data, directly or indirectly, from each of the sensors that monitor the network for the data specified in the CDM Program and for the objects within the dashboard’s scope via a database.

A Base CDM Dashboard will be used by organizations that own the objects in the scope of the dashboard, not only to monitor risk but to facilitate identification and removal of specific defects on specific objects.

CDM Dashboards will be connected through a hierarchy, with the Federal Dashboard at the top. Higher level dashboards will be capable of transferring meta-data to lower level dashboards. Lower level dashboards will be capable of passing data to the adjacent higher level dashboard. The aggregation process is needed by both small and large D/As. Large D/As may have multiple enclaves, each of which must have its own dashboard. The Government seeks to summarize the data up to and including the Federal level, which includes all executive branch civilian D/As**.** Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

RISK SCORES

A *risk score* for an individual defect is a numerical representation of the relative severity or importance of the finding to the risk for the system as a whole. Standardized scoring systems have been created for vulnerabilities (CVSS) and software weaknesses (CWSS); they have also been developed for configuration settings (CCSS), but these are not yet as widely accepted. Standardized scoring systems do not yet exist for other types of findings, such as unauthorized/unmanaged hardware, unauthorized software, anti-virus protection weaknesses, or data loss. A risk score for an IT asset represents the total measurable security risk associated with that asset. It combines standardized and non-standardized metrics with management heuristics and weightings to estimate the magnitude of risks and prioritize the allocation of resources for risk remediation. Risk scoring is a key element of the dashboard function, because it provides fair, objective, and repeatable quantitative comparisons among security risk elements that are not inherently comparable.

The lowest level scores are at the object/defect level. These can be summed to get the score for an object, the score for a defect across the entire D/A, or the total score for all objects in the D/A.

Each dashboard defines arbitrary groupings appropriate to the level of detail of its data and then report scores or findings by a selected grouping. Groupings of objects are used to assign risk scores to the sub-organizations that are directly responsible for, and able to actually remediate, findings. Groupings of defects facilitate their analysis prior to selection for remediation,
Each dashboard aggregates scores across any of the groupings to facilitate analysis for prioritization. Each dashboard calculates average risk scores and converts them into risk levels, e.g., letter grades, for appropriate groups of devices/objects, and provides group rankings based on average risk score compared to various reference groupings.

An aggregation process is needed by both small and large D/As, ranging from several hundred objects to millions of objects. Large D/As may have multiple enclaves and may want to operate the security configuration compliance assessment at the enclave level. Ultimately, the Government seeks to summarize the data up to and including the Federal level, which includes all civilian executive D/As**.** The lowest level of detail required for the Federal Dashboard is aggregate scores for object groups by defect check, e.g., the total score for all objects in a sub-organization for a specific vulnerability on a specific software product.

SITES

For a dashboard that contains data at the object level (Base and Intermediate Object-level CDM Dashboards), the objects should be organized into object containers called *sites* such that every object is in exactly one site. The scores assigned to the objects will be combined to provide a single score for the entire site. A site is intended to represent administrative ownership – the owner of the site is responsible for fixing the security issues associated with the site's objects. The case where responsibility for an object's scores is split among multiple owners is addressed by risk transfers.

SCORE TYPES

Scores are defined by sets of scoring parameters and are meant to be used by D/As to help prioritize the work of mitigating security defects. Each D/A must be able to tailor the scoring parameters to best accomplish this. However, at the Federal level, scores are meant to be used to assess the security posture of all the D/As and therefore the same scoring parameters must apply to all D/As. This is accomplished by using two separate sets of scoring parameters (one mandatory set for Federal scores and one optional set for D/A scores) throughout, although some D/As may wish to simply use the Federal parameters. Local D/A scoring, if desired, each D/A can assign these scores in whatever way meets their objective for using local scores, including different scores for different enclaves.

Scores are defined by sets of scoring parameters and are meant to be used by D/As to help prioritize the work of mitigating security defects. Each D/A must be able to tailor the scoring parameters to best accomplish this. However, at the Federal level, scores are meant to be used to assess the security posture of all the D/As and therefore the same scoring parameters must apply to all D/As. This is accomplished by using two separate sets of scoring parameters (one mandatory set for Federal scores and one optional set for D/A scores) throughout, although some D/As may wish to simply use the Federal parameters. If desired, each D/A can assign these scores in whatever way meets their objective for using local scores, including different scores for different enclaves.

The general scoring algorithm includes factors that take into account vulnerability score, threat multipliers, and impact multipliers. When using scores to evaluate risk, the inclusion of threat and impact is always appropriate. However, when using scores to grade performance, some multipliers may introduce perverse incentives and/or unfairness (particularly if local managers cannot mitigate the extra threat or impact), so the flexibility to ignore such multipliers may be useful. The dashboard should distinguish two kinds of "multipliers" (for both threat and impact): grade-relevant multipliers and non-grade-relevant multipliers. This produces two versions of the Federal and Local Scores: 1) a Grading Score (ignores the non-grade-relevant multipliers), and 2) a full-risk-score (includes all multipliers). The terminology shown on dashboard screens and reports these scoring types must be configurable to mitigate possible confusion with other D/A terminology. An end user must at any time be able to select display of scores using one of four scoring types: a) Federal-grading, b) Federal-Full-Risk, c) Local-grading, and d) Local-Full-Risk.

RISK TRANSFERS

To ensure that prioritization is limited to risks that can be directly remediated by the assigned organization, risk scores must be transferrable from one sub-organization to another at the object-defect level. For example, if an upgrade of a vulnerable version of Java Runtime Environment would break an application managed by another organization, the risk score for that vulnerability should be transferred to the organization that owns the application for every host that is used to run that application. Definition/approval of risk transfers is the responsibility of the D/A. Implementation of transfer rules is the responsibility of the D/A, who may delegate this to the CMaaS Contractor. Note that the dashboard must allow a D/A user to successfully implement risk transfers if they choose to do so. Risk Transfers are absolutely essential to maintaining a risk monitoring environment where risks can be fairly prioritized by the organizational level that is able to remediate the problems.

DEFECT

A *defect* is a security-related condition that represents a difference between a desired state and an actual state, e.g., a specific vulnerability in a software product or a user password set to never expire.

OBJECT

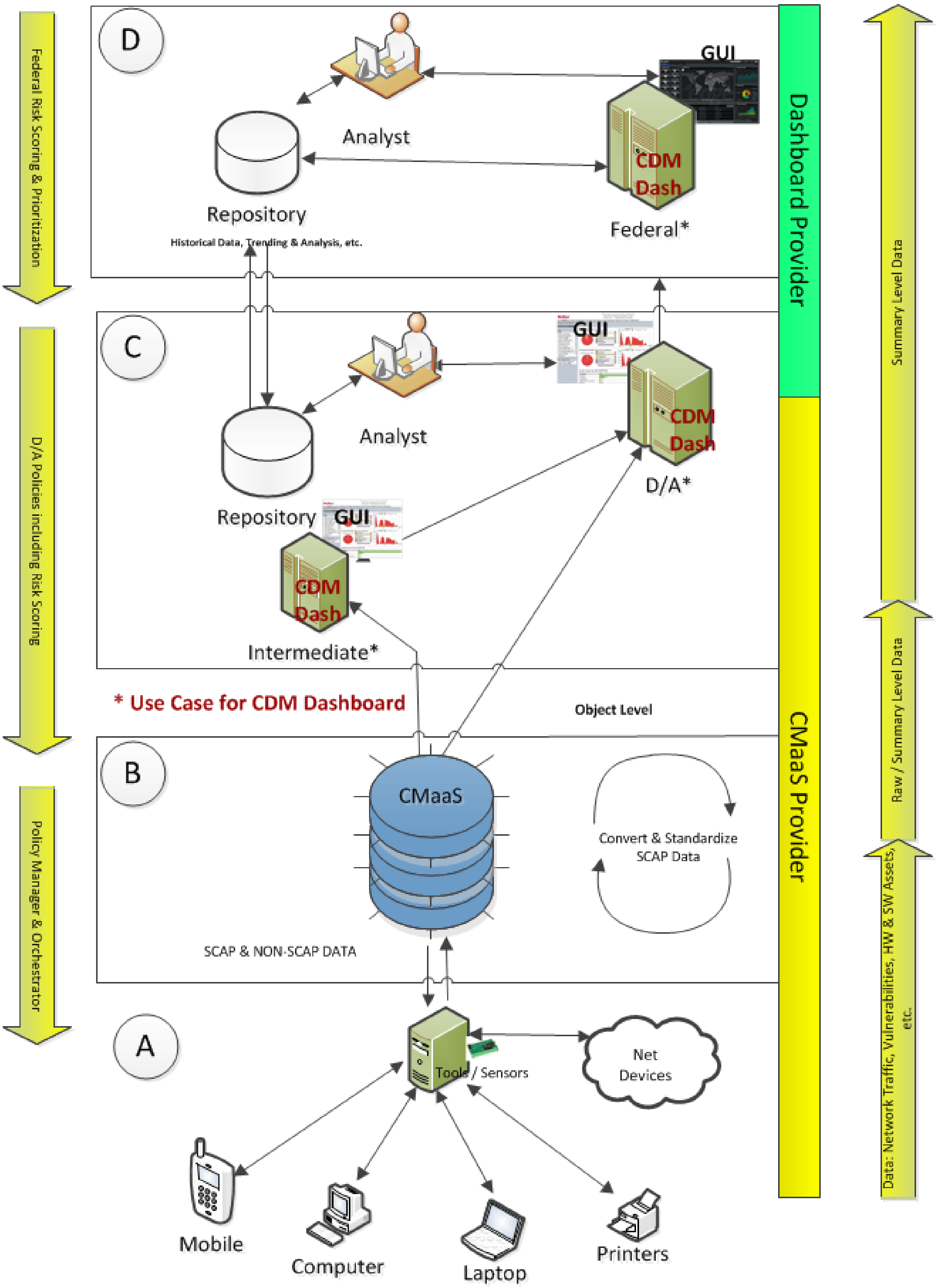
An *object* is anything that can have a defect. Generally, it is understood that an object is a network end point, e.g., a server, router, or workstation. However, a directory account will also be considered an object. In addition, objects form a hierarchy, i.e., one object can be contained in another object. For example, each software product installed on a server will be considered an object, but all such objects on a given server are contained in the object representing the server. Objects that are not contained within other objects will be called *root objects* where the distinction is important.

SENSOR

The term *sensor*, as used throughout this TOR, refers to the collection subsystem in the CAESARS-Framework Extension. The sensor concept includes both tools that collect data about endpoints on the network and the possibility of manually input data.

C.1.3.2 CDM Dashboard Architecture

The figure below shows the hierarchy possibilities.


Federal Risk Scoring & Prioritization
D/A Policies including Risk Scoring
Policy Manager & Orchestrator
D
Analyst
GUI
Repository
Historical Data, Trending & Analysis, etc.
CDM Dash
Federal*
Dashboard Provider
C
Analyst
GUI
Repository
GUI
CDM Dash
D/A*
CDM Dash
Intermediate*
* Use Case for CDM Dashboard
Object Level
B
CMaaS
Convert & Standardize SCAP Data
SCAP & NON-SCAP DATA
CMaaS Provider
A
Tools / Sensors
Net Devices
Mobile
Computer
Laptop
Printers
Summary Level Data
Raw / Summary Level Data
Data: Network Traffic, Vulnerabilities, HW & SW Assets, etc.

C.2 SCOPE

This procurement will obtain a single hierarchical CDM Dashboard solution with multiple use cases (Top/Federal Level, Intermediate Summary Level, and Intermediate Object Level). The Contractor shall design, develop, and support the implementation of a Dashboard Solution Interim Operating Capability (IOC) at the D/A levels (Intermediate Summary Level, and Intermediate Object Level); to a Full Operating Capability (FOC) for the Federal and all D/A level CDM Dashboards. The Contractor shall provide: analysis, DHS system engineering lifecycle (SELC) reviews, software development, testing, security accreditation support, implementation support (to include acquiring property), maintenance, documentation, configuration management, Tier 3 support, training, transition to support, and acquisition milestone tracking. The contractor will only implement the Federal use case of the CDM Dashboard, all other use cases will be implemented by CMaaS vendors. However, insofar as the Dashboard solution includes commercial or open-source software, the Contractor shall also provide to the Government, as part of this procurement, licenses to such commercial or open-source software in quantities sufficient both for the Federal implementation and to enable the Government to later provide such licenses to the CMaaS vendors for D/A implementations. Aspects of the CDM are classified TS/SCI and the contractor personnel supporting Task 5 – FOC Dashboard Implementation, of this effort will be required to work within classified space, handle TS/SCI Material, and participate in the TS/SCI efforts.

C.3 OBJECTIVES

The objectives of this Task Order (TO) are to develop an IOC and FOC tiered hierarchical dashboard capability for the Federal Government. DHS requires the pilot of the IOC at the D/A levels during CY 2014. The progression from IOC to FOC implementation may be done incrementally occurring over several software releases. Additionally, the FOC version is expected to have a software refresh cycle of every six months.

C.4 TASKS

C.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT (CLIN X001)

The Contractor shall provide program management support under this TO from TO Award (TOA) and project kick-off through transition-out. This program management shall include status reporting, status meetings, Project Management Plan, trip reports, Quality Control Plan, and Earned Value Management.

This includes the management and oversight of all activities performed by Contractor personnel, including sub-Contractors, to satisfy the requirements identified in this Statement of Work (SOW). The Contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality control, and leadership of the execution of this TO. The Contractor shall schedule meetings and provide deliverables in accordance with Section F.

C.4.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. The attendees shall include vital Contractor personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR. The Contractor shall provide the following at the Kick-Off meeting:

1. Project Management Plan (PMP)
2. Updated Quality Control Plan (QCP)
3. Updated Earned Value Management (EVM) Plan.

C.4.1.2 SUBTASK 1.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The Contractor PM shall develop and provide an MSR (Section J, Attachment B) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Federal Network Resilience (FNR) Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

1. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status.
4. Government actions required.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
7. EVM statistics.
8. Accumulated invoiced cost for each CLIN up to the previous month.
9. Projected cost of each CLIN for the current month.

C.4.1.3 SUBTASK 1.3 – CONVENE TECHNICAL STATUS MEETINGS

The Contractor PM shall convene a monthly Contract Activity and Status Meeting with the TPOC, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.4.1.4 SUBTASK 1.4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

1. Describe the proposed management approach
2. Contain detailed Standard Operating Procedures (SOPs) for all tasks
3. Include milestones, tasks, and subtasks required in this TO, to include granular detail, and all reoccurring deliverables (i.e. "New Code" and "Customizations", as defined in section C.4.12)
4. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
5. Include the Contractor's QCP and EVM Plan.

The Contractor shall provide the Government with a draft PMP at the project Kick Off meeting, on which the Government will make comments. The final PMP shall incorporate the Government's comments.

C.4.1.5 SUBTASK 1.5 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually and at the incorporation of any major task order modification. The Contractor shall work from the latest Government-approved version of the PMP.

C.4.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.4.1.7 SUBTASK 1.7 – UPDATE QUALITY CONTROL PLAN (QCP)

The Contractor shall update the QCP submitted with their proposal and provide a final QCP as required in Section F. The Contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified by the Government.

C.4.1.8 SUBTASK 1.8 - EARNED VALUE MANAGEMENT (EVM)

The Contractor shall employ and report on EVM in the management of this TO. See H.19, Earned Value Management**,** for the EVM requirements.

C.4.1.9 SUBTASK 1.9 – TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming Contractor/Government personnel at the expiration of the TO. The Contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of the TO. The Contractor shall identify how it will coordinate with the incoming Contractor and/or Government personnel to transfer knowledge regarding the following:

1. Project management processes.
2. Points of contact.
3. Location of technical and project management documentation.
4. Status of ongoing technical initiatives.
5. Appropriate Contractor–to-Contractor coordination to ensure a seamless transition.

6. Transition of Key Personnel.
7. Transfer of Software Licenses.
8. Schedules and milestones.
9. Actions required of the Government.

The Contractor shall also establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition via weekly status meetings.

C.4.2 TASK 2 – IOC Analysis of Design Alternatives (CLIN 0002)

Within four months of award the Contractor shall analyze at a minimum three alternative Commercial off-the-Shelf (COTS) or Open Source products that can meet as many of the IOC Dashboard requirements as possible for, at a minimum, the Base use case (see Section J, Attachments P and I). The IOC solution shall be based on COTS or Open Source product(s). The Contractor shall conduct an analysis of IOC Design Alternatives to include:

1. An analysis of dashboard requirements.
2. A gap analysis between the continuous monitoring information management needs for risk prioritization and reporting and the Government's current capabilities.
3. An analysis of existing dashboards and where they do not meet CDM reporting requirements, research potential incompatibilities, analyze system interfaces, and propose ways to resolve potential interface conflicts.
4. A comparison of alternative solutions and their capabilities for dashboard development and implementation (identifying Federal enterprise architecture constraints, if any).
5. A report that addresses at a minimum, the impacts on costs, engineering trade-offs, cost/benefit analysis, schedule dependencies, and technically feasible alternative approaches.
6. Exploration of possible solutions with the goal of identifying whether the required IOC dashboard capabilities currently exist in a commercial product, whether it exists but needs enhancements..
7. Sound rational for recommended approach.
8. Sound rational for rejection of alternatives.
9. Briefing for IOC Decision.

The Government will determine the best solution, based on the Contractor's analysis and recommendations. Once the decision is made, the Contractor shall create a written report on Design Alternatives and prepare an information briefing to be presented to DHS and D/A decision makers.

C.4.3 TASK 3 – Initial Operating Capability (CLIN X001)

The Contractor shall develop/procure an Initial Operating Capability (IOC) for the D/A level Dashboards. The IOC shall be based on Government selected solution from Task 2. It shall be used to provide an initial dashboard capability while the Full Operating Capability (FOC) D/A level and Federal Dashboards are being developed

C.4.3.1 SUBTASK 3.1 – IOC Systems Engineering Life Cycle (SELC) Compliance

The Contractor shall perform all systems engineering, architecture and testing tasks in this SOW in accordance with DHS AD 102-01/SELC. The Contractor shall provide best practices, technologies, tools, and support to quality and operational assessments, integration testing and system test and evaluation, including development of security certification and accreditation packages for agencies for the dashboards. DHS, with vendor support, will develop one package that can be provided for all D/A's to use. All development and testing will take place at the vendors facilities, utilizing the vendors equipment with Government access to the location and all artifacts made available to the Government. If required, the Contractor shall participate in and support an IV&V to ensure the monitoring and evaluation of projects through activities such as, but not limited to, assessments, process and procedure audits, project and performance management, and systems analysis and design. IV&V testing shall be in accordance with the DHS SELC.

The DHS SELC framework is used across all DHS systems; it will be the only SELC framework model to be followed. DHS may elect to have stakeholders from D/A as participants in the various reviews, most likely the Operational Readiness Reviews into their environment.
It consists of nine process stages and corresponding Systems Engineering Reviews: Solution Engineering, Planning, Requirements Definition, Design, Development, Integration & Test, Implementation, Operations & Maintenance, and Disposition. SELC stage entry and exit criteria completion (as well as technical progress) are validated in the stage reviews. Solution Engineering focuses on enterprise level activities. The remaining stages address project and system related activities. The Contractor shall provide support across all phases of the SELC, including engineering review and SELC stage specific activities as required.

The stages and reviews may be repeated by projects during capability implementation. The stages and activities may be tailored by the program, as not all projects will require all stages in the SELC and others may require multiple iterations. Minor system modifications and enhancements during O&M will not require all stages of the SELC to be performed. Major enhancements will be treated as new projects within the SELC.

The Contractor shall follow a tailored approach to the acquisition milestone review process, in accordance with DHS Acquisition Directive 102-01.

The Contractor shall produce DHS SELC Documentation and Briefing Materials and participate in the following four design reviews for the IOC Dashboard.

1. Solution Engineering Review (SER),
2. Project Planning Review (PPR),
3. Critical Design Review (CDR), and
4. Production Readiness Review/Operational Test Readiness Review (PRR/OTRR).

C.4.3.2 SUBTASK 3.2 – Provide the IOC Solution for D/As

The Contractor shall implement the Initial Operating Capability. This implementation shall include Systems Engineering Life Cycle Compliance, DHS Enterprise Architecture Compliance, Security Accreditation, Maintenance Support, and Dashboard IOC Documentation. The Contractor shall provide the following:

1. Provide and tailor the Government-approved dashboard solution.
2. Perform reviews to identify technical and operational issues and problems such as requirements definition, architecture and policy compliance, and engineering guideline development including peer-to-peer reviews, code walk-throughs, and formal design reviews.
3. Recommend opportunities for resolving issues in requirements, data, applications, and infrastructure elements.
4. Coordinate with the CMaaS Contractor(s) or other Government-designated integrators for the engineering and integration of the Dashboard solution with computer system, hardware, operating software, and networks.
5. Provide analysis, modeling, design, development, enhancements, testing, and documentation of new and existing capabilities. The Dashboard solution shall be subject to formal Government and end-user acceptance test in accordance with approved test plan and procedures (which shall be consistant with the CDM Test Evaluation Master Plan (TEMP) definitions.
6. Conduct an extended development test (EDT) within a DHS supplied environment prior to completion of the production-ready D/A Dashboard solution.
7. Production ready IOC solution is handed off to CMaaS vendor for implementation.
8. After the IOC Dashboard solution is operational, the Contractor shall provide enhancements to existing software application programs throughout the period of performance; develop work-arounds to the IOC Dashboard based on Government approved requirements; and provide a software release every 6 months until FOC is achieved.

The Contractor shall establish associate Contractor agreements with the CMaaS Contractor(s) or other integrator for cooperative co-maintenance of dashboard software. Object containers, object types, defect checks and defect groups can all be defined locally, as can scoring parameters. Impact factors can be defined at the object level even if local scoring is not used. Additional user-level customizations may be required at individual D/As.

C.4.3.3 SUBTASK 3.3 – IOC Security Accreditation

The IOC Dashboard solution will be a DHS asset. The DHS will perform the security accreditation and the D/A will perform a risk acceptance. The Contractor shall provide input and facilitate the execution of Memoranda of Agreement (MOAs) between DHS and the D/A for risk acceptance in a support capacity to DHS. The Contractor shall ensure that C&A is received from DHS before the IOC capability is installed on a DHS network. The Contractor shall provide all support required to ensure that the Dashboard passes the DHS security accreditation process. The IOC Dashboard shall be subject to continuous monitoring and reaccreditation every three years. The Contractor shall support the third party performance of the security accreditation tests against the system. The Contractor shall ensure that the IOC Dashboard solution remains accredited in accordance with DHS security guidelines (4300 A, DHS Sensitive Systems guidelines). The Contractor shall perform the following security authorization tasks:

1. Provide the necessary support for security authorization of the Federal Dashboard community.
2. Provide support for the DHS accreditation process in accordance with applicable DHS standards.
3. Prepare documentation in support of the DHS accreditation process.

C.4.3.4 SUBTASK 3.4 –IOC Maintenance Support

The Contractor shall establish and manage a comprehensive Maintenance Program that includes IOC Dashboard solution installation support, connections, access control, configurations and inventory of components. The Contractor shall provide comprehensive support, including:

1. Dashboard policies, procedures, and guidance.
2. Dashboard implementation packages and guidance.
3. Scheduled maintenance.
4. Unscheduled maintenance.
5. COTS/OPEN SOURCE CODE Product upgrades.
6. Planned and integrated logistics support for Dashboard components.
7. Integration of new technology.
8. Information security.

D/A level dashboard software and hardware will be installed and integrated by CMaaS Contractor(s) or other Government-designated integrators and the Dashboard Contractor shall provide technical advice and support as needed.

C.4.3.5 SUBTASK 3.5 – IOC DHS Enterprise Architecture Compliance

To the maximum extent possible, the Contractor’s IOC Dashboard solution shall meet DHS Enterprise Architecture policies, standards, and procedures. However, the mission of the CDM program is to service the entire Federal Executive Civilian branch (.gov Domain), and its Enterprise Architecture requirements must be viewed from that broader perspective. As such, there may be instances in which the CDM Architecture may need to deviate from and/or extend Homeland Security (HLS) Enterprise Architecture (EA) requirements. The Contractor shall comply with the following Homeland Security (HLS) EA requirements with regard to the IOC Dashboard:

1. The IOC D/A dashboard shall be compliant with the Federal enterprise architecture. Specific compliance issues should be treated as a defect to be considered for the next release.
2. IT hardware and software deployed on DHS networks shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
3. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

4. Development of data assets, information exchanges and data standards shall comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts shall be developed and validated according to DHS data management architectural guidelines.
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related elements (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

C.4.3.6 SUBTASK 3.6 – IOC Dashboard Documentation

All IOC Dashboard software releases shall be accompanied with documentation updates including Release Notes and Release Implementation Guidelines, page updates (one copy per site) and paperless electronic on-line Dashboard User Manual, and Operations Manual updates. The Release Notes and Release Implementation Guidelines shall include descriptions of what has changed in the new release and how to install the new release(s), including installation requirements for particular sites. The documentation shall include a description of functional changes for all releases. The Contractor shall provide the documentation in coordination with scheduled block release dates.

C.4.4 TASK 4 – FOC Requirements Validation and Design Alternatives (CLIN X003)

Within 12 months of award the Contractor shall validate the Dashboard solution requirements and develop FOC design alternatives for Government decision.

C.4.4.1 SUBTASK 4.1 – FOC Requirements Validation

The Contractor shall conduct an analysis and document validation activities that include, but are not limited to, the following:

1. Analysis of the production environment (D/A CDM Dashboard connected to the live D/A feeds of their network).
2. Analysis of existing and new sensors and dashboard capabilities.
3. Analysis of system interfaces.
4. Identifying potential interface incompatibilities.
5. Resolving interface conflicts.
6. Ensuring that the Dashboard solution will meet the constraints of DHS Enterprise Architecture.

The Contractor shall compile a list of potential solutions for the FOC Dashboard requirements. Following Government review of the design alternatives, the Contractor shall procure, test and evaluate those platforms that the Government identified as best meeting its need.

C.4.4.2 SUBTASK 4.2 – FOC Design Alternatives

Based on the validated requirements in subtask 4.1, the Contractor shall design alternative approaches to meet the FOC CDM Dashboard requirements for Government selected platforms. Building on the IOC Analysis of Design Alternatives (Task 2), the Contractor shall conduct an analysis of FOC Design Alternatives to include:

1. Analytical comparison of alternative solutions and their capabilities for dashboard development and implementation.
2. Conceptual solutions with the goal of identifying whether the IOC solution needs enhancements, or if it must be a new custom developed tool that may or may not utilize portions of existing tools.
3. Rational for recommended approach.
4. Rational for rejection of alternatives.
5. Presentation of FOC Design Alternatives

After presenting the FOC Design Alternatives, the Government will make a select the solution that best meets its requirements. Once the decision is made, the Contractor shall create a written report on the FOC Design Alternatives and prepare an information briefing to be presented to DHS and D/A decision makers.

C.4.5 TASK 5 –FOC Dashboard Implementation (CLIN X001)

The Contractor shall implement the FOC Dashboard Federal use case within 24 months after approval of FOC recommendations. This implementation shall include SELC Compliance, DHS Enterprise Architecture Compliance, Security Accreditation, Maintenance Support, and Dashboard FOC Documentation. The Contractor shall provide FOC capabilities for D/A use cases, and integrate a FOC Federal use case CDM Dashboard, based on the Government’s decision from the Alternatives Briefing in Task 4.2. The FOC Dashboards shall meet as many of the requirements as possible (see Section J, Attachments P and I). The Contractor shall provide software development, functionality enhancement (progressive versions), and maintenance support for Dashboard(s) as approved by the Government. The Contractor shall develop a software development process that employs best industrial practices including integration, testing, and documentation of software. Object containers, object types, defect checks and defect groups can all be defined locally, as can scoring parameters. Impact factors can be defined at the object level even if local scoring is not used. Performance on this contract will requires support personnel to access information up to and including Top Secret and Sensitive Compartmented Information (SCI). Contractor staff supporting Task 5 that will require access within the hosting environment (in relation to the Federal CDM Dashboard instance only) of this contract are required to hold and maintain a Top Secret SCI clearance.

C.4.5.1 SUBTASK 5.1 – FOC Systems Engineering Life Cycle Compliance

The Contractor shall perform all systems engineering, architecture and testing tasks in this PWS in accordance with DHS AD 102-01/SELC. The Contractor shall provide best practices, technologies, tools, and support to quality and operational assessments, integration testing and system test and evaluation, including development of security certification and accreditation packages for agencies for the dashboards. If required, the Contractor shall participate and support an IV&V to ensure the monitoring and evaluation of projects through activities such as, but not limited to, assessments, process and procedure audits, project and performance management, and systems analysis and design. IV&V testing shall be in accordance with the DHS SELC.

The DHS SELC framework is used across all DHS systems. It consists of nine process stages and corresponding Systems Engineering Reviews: Solution Engineering, Planning, Requirements Definition, Design, Development, Integration & Test, Implementation, Operations & Maintenance, and Disposition. SELC stage entry and exit criteria completion (as well as technical progress) are validated in the stage reviews. Solution Engineering focuses on enterprise level activities. The remaining stages address project and system related activities. The Contractor shall provide support across all phases of the SELC: including engineering review and SELC stage specific activities as required.

The stages and reviews may be repeated by projects during capability implementation. The stages and activities may be tailored by the program, as not all projects will require all stages in the SELC and others may require multiple iterations. Minor system modifications and enhancements during O&M will not require all stages of the SELC to be performed. Major enhancements will be treated as new projects within the SELC.

The Contractor will follow a tailored approach to the acquisition milestone review process, in accordance with DHS Acquisition Directive 102-01. For the FOC Dashboards the Contractor shall provide the documentation, briefing materials, and presentations for the following DHS SELC reviews:

1. Solution Engineering Review (SER).
2. Project Planning Review (PPR).
3. Systems Definition Review/Preliminary Design Review (SDR/PDR),
4. Critical Design Review (CDR).
5. Integration Readiness Review/Development Test Readiness Review (IRR/DTRR).
6. Production Readiness Review/Operational Test Readiness Review (PRR/OTRR).

The Contractor shall provide subject matter expertise on the FOC Dashboards for the Operational Readiness Review (ORR) and the Post Implementation Review (PIR). The actual reviews will be conducted by another Contractor tasked with installation of the FOC Dashboards.

C.4.5.2 SUBTASK 5.2 – FOC DHS Enterprise Architecture Compliance

To the maximum extent possible, the Contractor’s dashboard solution shall meet DHS Enterprise Architecture policies, standards, and procedures. However, the mission of the CDM program is to service the entire Federal Executive Civilian branch (.gov Domain), and its Enterprise

Architecture requirements must be viewed from that broader perspective. As such, there may be instances in which the CDM Architecture may need to deviate from and/or extend Homeland Security (HLS) EA requirements. The Contractor shall comply with the following Homeland Security (HLS) EA requirements with regard to dashboard:

1. The developed FOC solution shall be compliant with the Federal enterprise architecture and may need to follow specific D/A EA guidelines when deployed as identified, and provided by DHS.
2. IT hardware and software to be deployed on DHS networks shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
3. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
4. Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related elements (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

C.4.5.3 SUBTASK 5.3 – FOC Security Accreditation Support

The FOC Dashboard software will be a DHS asset. The DHS will perform the security accreditation and the D/A will perform a risk acceptance. The Contractor shall support the D/A with regard to the execution of Memoranda of Agreement (MOAs) with the D/A for risk acceptance. The Contractor shall ensure that C&A is received before the FOC capability is installed on a DHS network. The Contractor shall provide all support required to ensure that the Dashboard passes the DHS security accreditation process. The Government also expects that the FOC Dashboard, as part of a CMaaS deployment, must be subject to continuous monitoring and reaccreditation every three years. The Contractor shall run tests against the system. The Contractor shall ensure that the FOC Dashboard system remains accredited in accordance with DHS security guidelines (4300 A, DHS Sensitive Systems guidelines).

The Contractor shall perform the following security authorization tasks:

1. The Contractor shall provide the necessary support for security accreditation of the CDM Dashboard community.
2. Provide support for the DHS accreditation process in accordance with DHS standards.

3. Prepare documentation in support of the DHS accreditation process.

C.4.5.4 SUBTASK 5.4 – FOC Maintenance Support

The Contractor shall establish and manage a comprehensive Maintenance Program that includes for all use cases; connections, access control, configurations, inventory of dashboard components, and installation of the Federal CDM Dashboard use case. The Contractor shall provide comprehensive support, including:

1. Dashboard Policies, procedures, and guidance.
2. Dashboard implementation packages and guidance.
3. Scheduled maintenance.
4. Unscheduled maintenance.
5. Planned and integrated logistics support for Dashboard components.
6. Integration of new technology.
7. Information security.

D/A CDM Dashboard use cases will be installed, implemented, and operated by CMaaS Contractor(s) or other integrator(s).

C.4.5.5 SUBTASK 5.5 – FOC Documentation of Dashboard Build

All software releases shall be accompanied with documentation updates including Release Notes and Release Implementation Guidelines, page updates (one copy per site) and paperless electronic on-line Dashboard User Manual, and Operations Manual updates. The Contractor shall provide the documentation to the sites and to DHS, in coordination with scheduled block release dates. The Release Notes and Release Implementation Guidelines shall include descriptions of what is taking place in the new release and how to install the new release(s), including installation requirements for particular sites. They shall include:

1. A description of functional changes for all releases,
2. Current and new sensors and dashboards.
3. System interfaces.
4. Resolving interface conflicts.
5. Ensuring that systems meet the constraints of systems architecture(s).

C.4.6 TASK 6 – Customer Support (CLIN X001)

Customer Support shall include Tier Three help support and training support to ensure the highest state of reliability for the Federal Dashboard and related dashboards.

C.4.6.1 SUBTASK 6.1 – Tier 3 Support

The Contractor shall provide Tier Three Support for the Dashboard User Community for IOC and then FOC. The Contractor shall provide a ticketing system and hot-line capability during the normal workweek (Monday through Friday) and shall provide coverage from 0700 through 1700 hours Eastern time daily (normal work week).

1. Tier One support will be provided by the D/As. Tier One support shall include Problem resolution using standard methodologies and basic troubleshooting techniques.
2. Tier Two support will be provided by CMaaS Contractor(s) or Government-designated integrators. Tier Two support shall include more in-depth troubleshooting and shall require specialized knowledge of sensors and dashboards for remediation.
3. All calls determined by Tier Two to be related to the dashboard solution and not resolved through Tier Two shall be forwarded to the Dashboard Contractor for Tier Three support.

The Contractor shall provide systems engineering support necessary to establish and maintain a hot-line support capability. The Contractor shall refer technical issues to appropriate technical personnel and provide technical assistance.

The Contractor shall establish a procedure for recording and tracking all requests for operational support. All requests for operational support shall be reviewed and prioritized by the DHS Program Office. The Contractor shall, as a minimum, provide the following support:

1. Provide initial problem resolution where possible.
2. Generate, monitor, and track open Incident Reports through resolution and report the statistics to DHS.
3. Provide software support.
4. Record problem resolution.
5. Maintain frequently asked questions and their resolutions.
6. Obtain customer feedback and conduct surveys.

C.4.6.2 SUBTASK 6.2 – FOC Training

The Contractor shall develop operational training plans and associated training materials, and conduct operational training. The training plans shall outline the personnel to be trained, a schedule for training and shall show graphical representations of the screens of the developed/modified systems. The Contractor shall provide the following:

1. Development of education, training and awareness briefings, and articles.
2. Maintain employee participation status.
3. Prepare security education, training and awareness materials.
4. Provide training to CMaaS vendors.

The Contractor shall develop a training program that addresses proper transmittal of sensor data to the dashboard, how to establish and maintain a dashboard link, basic dashboard operations. The Contractor shall provide the training onsite or at designated locations nationwide, TBD by the COR.

C.4.7 TASK 7 – CDM Acquisition Milestone Tracking System (CLIN X001)

The Contractor shall maintain a system to track the CDM dashboard project as it proceeds through each SELC milestone. This CDM Acquisition Milestone Tracking System shall identify, schedule, and report on the progress of meeting review entrance and exit criteria and completing program artifacts.

The electronic tracking system shall identify all of the required documents for delivery/ presentation to each DHS Review Authority, along with tracking the scheduled start and completion dates and the actual start and completion dates for preparation, review, and approval of each document. The system shall also identify, for each document, the document name and identification number; version number; date; organization; and the specific person in that organization responsible for completing the preparation, review, and approval of each document.

The Contractor shall prepare and deliver a monthly report providing the status of the program's progression through the acquisition milestones. For an FNR-sponsored project that is entering into an acquisition milestone review, the report should include a summary of the status of the required artifacts and indicate which artifacts may require attention prior to the review.

In addition to the DHS acquisition reviews, the Contractor shall support the Government in developing and supporting FNR-internal program capability reviews by providing relevant CDM Acquisition Milestone Tracking System output. These reviews will be performed in preparation for submitting program documents to the Systems Engineering Lifecycle, Enterprise Architecture, and Acquisition Review Boards.

C.4.8 TASK 8 – Testing Support (CLIN X001)

The Contractor shall provide testing support for all scheduled software releases (IOC, FOC, and future updates). The Contractor shall prepare functional testing and coordinate with DHS for system acceptance on all system upgrades and software releases. All results and problems tracked through customer support shall be logged and reported to FEDSIM and DHS upon request and in the monthly report.

The Contractor shall prepare test plans and procedures which shall provide for user acceptance testing of functional enhancements for all major releases of the Dashboard. Major releases shall be identified by incremental increases in either the first or second position of the release number (i.e., 2.0, 2.1, 3.1). Minor releases shall be identified by incremental numbering following the first two positions of the release number (i.e., 2.1.1, 1.1.0.5).

The Contractor shall support the CDM Dashboards by providing interface testing, integration testing, preparation of test plans and procedures, test reports, acceptance testing, and demonstration activities of products targeted for and used by CDM Dashboards.

System testing and laboratory support shall include, but not be limited to, testing support through final acceptance testing of targeted applications; testing for scalability, conducting integration testing of hardware, software, and/or data communications enhancements; and providing support for and liaison with system maintenance, configuration management and control activities for new and existing dashboard applications.

The Contractor shall provide an Integration Test and Evaluation (IT&E) capability that is capable of the development, deployment, and ongoing support of the information systems that now and in the future will comprise the CDM Dashboard.

The Contractor shall establish a testing capability/process and provide support to ensure that all integrated applications are compatible and interoperable with all deployed Dashboard components prior to installation on the Dashboard.

The Contractor shall prepare a Test and Evaluation Master Plan (TEMP) that provides the Contractor’s conceptual approach for delivering quality products to include critical test parameters, evaluation criteria, developmental test and evaluation methods, operational test and evaluation methods, automated test tools, and resource management. The Contractor shall identify sets of the testing tools to implement in the test environment. The Government must approve the test plans prior formal testing. The Contractor shall follow this approved Master Plan throughout the task order to produce test plans and reports. The initial TEMP shall be delivered to TPOC and the FEDSIM COR within 30 work days after the Government makes their approach decision.

The Government and/or its representatives (operational test authority [OTA] , Independent Verification and Validation Team [IV&V] for example) shall be allowed to observe any developmental /operational test and evaluation conducted by the Contractor. The Government and/or its representatives (OTA, IV&V etc) shall be able to review the Contractor’s test plan(s) with sufficient time to comment and have comments incorporated by the Contractor into the test plan as appropriate. The Contractor is expected to participate in integrated project teams for test and evaluation. The Government reserves the rights to conduct an operational and security related assessments of the Dashboard with users involved, with the full cooperation of the Contractor. Results from these security/operational assessment shall be used to provide feedback to the Government program office as to how the dashboard is proceeding towards meeting security/ operational requirements.

C.4.9 TASK 9 – Configuration Management (CLIN X001)

C.4.9.1 SUBTASK 9.1 – Configuration Management Support

The Contractor shall provide Configuration Management of the Federal and D/A Dashboard systems, to include hardware, software, and networks. The Contractor shall use industry best practices to provide configuration identification, configuration control, configuration status accounting, and configuration review/audit services. The Contractor shall conduct the following configuration management activities as a minimum:

1. Use the appropriate Configuration Management tool to account for changes made IAW the Configuration Management process. The Configuration Management tool shall account for Federal Dashboard assets, software and hardware, and status

accounting to include, as a minimum: Maintain hardware and software accountability and configuration change records for all Federal Dashboard hardware and software assets by make, model, and serial number; Maintenance history; Warranty information; License information; and Configuration change information.

2. Work directly with requesters and technical support personnel to gather sufficient background information to ensure proposed solutions meet customer needs and requirements.
3. Record and report change processing and implementation status throughout the system life-cycle (hardware and software).
4. Ensure proper licensing for software in use on supported systems and networks and maintain a system of licensing accountability and internal control procedures.
5. Provide technical assistance in configuring, testing, and recommending software, hardware, and network management utilities.

C.4.9.2 SUBTASK 9.2 – Prepare Configuration Management Plan

The Contractor shall prepare a Configuration Management Plan to identify and define the organization and responsibilities, overall tasks, principles, and configuration management processes for the Dashboard. The purpose of Configuration Management Plan is to ensure a coherent view of a compatible method and procedure for configuration management of the system and its comprising subsystems, and provide emphasis on a disciplined integrated configuration management approach. The Configuration Management Plan shall establish the processes to manage changes in documentation, systems, hardware configuration items, and software configuration items. It shall define the Configuration Management organization and responsibilities, define the baselines to be tracked, and address the four major activities of Configuration Management: configuration identification, configuration control, configuration status accounting, and configuration auditing functions. The Contractor shall provide this CM support in conjunction with the Government Change Control Boards (CCBs) at the Federal and D/A levels.

C.4.10 TASK 10 – Software Changes (CLIN X001)

The Contractor shall provide on-going support to maintain and improve the functional processes within Dashboard software as prioritized and approved by DHS and the FEDSIM COR. These requirements shall consist of maintenance requirements, feature clarifications, modifications, and deficiency reports submitted and prioritized and approved by DHS. The Contractor shall provide support for all phases of project life cycle, including analysis, design, and program code, testing, and implementation, for the approved Dashboard maintenance, feature clarifications, modifications, and approved deficiency requests. The Contractor shall conduct and/or participate in design approval reviews and provide documentation updates to reflect functional and operational impacts and alternatives. All changes will have to be reviewed including COTS/Open Source Code software patch and revision updates. The Contractor shall provide a software version release every six months, or as required by the Government.

C.4.11 TASK 11 – Contractor Acquired Property (CLINs X001 and X005)

The Contractor shall acquire IOC Dashboard IT assets, e.g., equipment, software, and services in support of the IOC Dashboard. Upon receipt of Government approval, the following categories of information technology assets shall be procured by the Contractor: software, hardware, upgrades, licenses, and spare parts as required, in accordance with the terms of paragraph H.5 of the Alliant SB basic contract. The Contractor shall ensure that all hardware provided includes the most cost-effective warranty available from the vendor. In most cases, warranty coverage should be for parts only versus on-site warranty coverage.

C.4.12 TASK 12 – Source, Object, Executable and Run-time Code (CLIN X001)

The Contractor shall provide the most current version(s) of any and all source, object, executable and run-time code (as applicable) developed under the efforts of this contract ("New Code") for the IOC and FOC Dashboard Solutions and unique enhancements, customization/plug-ins/etc ("Customizations") to the Government in accordance with the delivery requirements in section F.5. The Government's requirements for data rights in the New Code and Customizations are specified in sections H.25.6, H.26, H.27, L.8.7 and M.5.1(c) and FAR clause at 52.227-17, Rights in Data – Special Works (Jun 1987). The Contractor shall ensure that all COTS licenses, and Open Source licenses both allow for the creation of the New Code and Customizations and vest the data rights to the New Code and Customizations exclusively in the Government, in both cases without additional charge to the Government. DHS will have unlimited rights to use and modify all source, object, executable and run-time code (as applicable) comprising the New Code and Customizations, and its associated documentation, even in the event that the Contractor should become unable to continue supporting the Dashboard, and the Contractor shall deliver each deliverable accompanied by a signed assignment of copyright to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Jun 1987). Source, object, executable and run-time code (as applicable) comprising the New Code for releases of the software produced under this contract shall become the property of the Government upon termination of the contract. The source, object, executable and run-time code (as applicable), with their associated documentation and other materials as specified in section F.5, shall be delivered to DHS on dates established in accordance with section F.5, but in any event no later than 30 calendar days following the termination/expiration of the contract. In the event the Contractor defaults on the terms of this contract for any reason, the most current version of the source, object, executable and run-time code shall be delivered to DHS no later than 30 calendar days following the event that leads to the termination/expiration of the contract and the Government will retain the right to use any and all versions that are at that time installed at a Government facility, and to further develop and distribute them, with no further royalties or other payments being due to the Contractor or any other party.

C.4.13 TASK 13 – Transition to Support Plan (CLIN X001)

The Contractor shall develop and deliver a Transition to Support Plan that documents how the FOC Dashboard solution will be operated and supported (once it is transitioned to the Government and/or a third party who will be operating and maintaining it). The FNR Operations group will manage the transition to support process for the Government. The Transition to Support Plan shall address the following:

1. Deployment schedule/milestones.
2. Required support resources.
3. Deployment tasks that require system administration support.
4. Security “clean bill of health” (required scan results, remediation POA&Ms, etc.).
5. Detail DHS Technical Reference Model (TRM) actions.
6. System architecture diagram(s).
7. Testing Results.
8. Readiness Activities.
9. Training resources.
10. System demonstrations.